REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Claim 17 is currently being amended.

This amendment adds, changes and/or deletes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 1-41 are now pending in this application, of which claims 34-41 were previously withdrawn.

Independent claim 17 has been amended to add a further limitation that the configuration files that the secure network interface is configured to receive and that the agent module is configured to implement are node-specific configuration files. Support for this amendment can be found within the originally filed application at least at ¶0011 and original independent claims 1 and 21. No new matter is added by way of the present amendment.

Applicants' invention is directed to implementing secure communications to ensure security of sensitive assets, such as shipping containers. A system according to the invention includes multiple remote nodes, each including a processor, storage means, and a set of detector interfaces configured for coupling to a set of detectors. Detectors detect an illegal condition, such as presence of one or more suspicious materials, suspicious activity, etc., to ensure security of sensitive asset. Because sensitive assets, such as shipping containers, are handled by potential adversaries for extended periods of time, special provisions are required to ensure security of the asset.

Applicants' invention as described in ¶0011 provides a secure network in which at least one node therein generates and distributes to each node an intelligent agent module and a set of

node-specific configuration files. In particular, these configuration files include information defining for that node a set of other nodes with which the node can communicate. Once installation is complete, security can be enhanced by encryption means (e.g., key pairs) implemented between nodes. In some embodiments, strobing of the encryption means (e.g., changing encryption keys every 30 to 60 seconds) is provided to further enhance security. The ability to configure and reconfigure the remote nodes, particularly when combined with encrypted communications therebetween, provides flexibility within the secure network thereby ensuring security of the sensitive asset.

As recited in Applicants' independent claim 1:

> A secure detection network system having a plurality of nodes, each node comprising a processor and storage means, the system comprising ... at least one server node configured to initialize and install each remote node in the plurality of remote nodes, including delivering to each remote node an agent module, said agent module for each remote node comprising a node specific configuration file. (Emphasis added).

Independent claim 21 recites similar limitations. Independent claim 17 as amended herein is directed to a secure detection node similarly reciting "a secure network interface, configured to receive an agent module and node-specific configuration files."

Turning briefly to U.S. Patent No. 6,532,166 to Mishra et al. (Mishra et al.) cited in the Office Action, a method and system is described for installing software implementations, such as applications and COM classes, as they are needed from an external source such as a centralized network store. (Abstract). As further described in col. 2, lines 9-16, the operating system receives a request corresponding to a software implementation. The system and method determines from the information whether the software implementation is locally installed on the computer system, and if not, it is installed from a network source, if available.

Mishra et al. describes on demand installation of applications for purposes of application deployment. (Col. 5, lines 41-65). One or more group policy objects (templates) may be

associated with policy recipients, and a sub-container of each group policy object (a class store 70) may include application deployment information. In an example illustrated in FIG. 7 and FIG. 8 and described at col. 6, line 27 through col. 7, line 13, an operating system shell 85 of a client workstation (FIG. 4) looks to a local registry for an application supporting a user's request. If not found, the operating system next looks to find the particular application in an Active Directory 66 maintained on a remote domain controller (see FIG. 3). If found, the application is effectively assigned to the user.

Turning next to U.S. Patent No. 5,642,394 to Rothschild (Rothschild) cited in the Office Action, an enhancement X-ray imaging system for detecting an object, such as an object being inspected for detection of any illegal materials. (Col. 2, line 66 through col. 3, line 2). The system includes a processor 18 connected to two detectors 14, 16 and receiving electrical signals therefrom. The system also includes a video display 20 connected to the processor for producing a visual image including a representation of a portion of any illegal materials. (Col. 3, lines 21-32).

Claim Rejections Under 35 U.S.C. § 103

Claims 1, 3-6, 13-18, 7-10, 19-21, 23-31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mishra et al., in view of McDaniel et al. and further in view of Rothschild. Applicants traverse for reasons set forth below.

With respect to independent claim 1, the above combination of references fails to render Applicants' invention obvious, because even if the references are combined as suggested in the Office Action, the combination still fails to teach or suggest every limitation of the claim.

First, contrary to Examiner's assertion, Mishra et al. fail to describe, teach, or suggest at least the limitation of a server node "delivering to each remote node an agent module for each remote node comprising a node specific configuration file" (emphasis added) as recited in Applicants' claimed invention. The portion of the reference cited by the office action (col. 5, lines 40-65) refers to one or more group policy objects (templates) 62 that may be associated

with policy recipients. The Office Action fails to explain how this makes obvious "delivering to each remote node an agent module for each remote node comprising a node specific configuration file."

As acknowledged in the last paragraph of page two of the Office Action, Mishra et al. describe a method and system for installing software implementations, such as applications as they are needed from an external source such as a centralized network store. To accomplish this, Mishra et al. describe an on-demand install mechanism 84 and a class store manager 86 (see FIG. 4) resident on the workstation (i.e., remote node). The domain controller 68 (FIG. 3) (i.e., server node) includes an Active Directory 66 with class stores 70. As described at col. 7, lines 1-12, the on-demand install mechanism 84 calls the class store manager 86 to query class stores 70 on the server node. If a requested application is found, the application is effectively assigned to the user, the registry is populated, and the item is added to a Start Menu. In other words, the remote node performs a directory look up on the server node. If the look up is successful, information returned to the remote node is used to assign the requested application to a user's profile. There is nothing in Mishra et al. to teach or suggest that the information returned to the remote node is a node-specific configuration file, as claimed. Thus, the reference does not appear to establish that an on-demand software implementation involves a node-specific configuration file.

The Office Action correctly observes that Mishra et al. fail to include defining a set of nodes with which the remote node can communication and different encryption means corresponding to each node. The Office Action relies on McDaniel et al. to provide these features.

McDaniel et al. describe a method and system for determining and enforcing security policy in a communication session are provided in distributed systems. (Abstract). McDaniel et al. is directed to group communication, describing at ¶0006 that properties required by a session are defined through a group policy. McDaniel et al. describe at ¶0123 that the policy states a basis set of mechanisms to be configured for the group. For example, at ¶0135 McDaniel et al.

describe the local member accepts any authorization and access control model defined by the group policy. Thus, McDaniel et al. is directed to groupings that can benefit from group policy. Nowhere does McDaniel et al. describe delivering to each remote node an agent module, said agent module for each remote node comprising a node specific configuration file, as recited in Applicants' claims. Accordingly, McDaniel et al. fails to cure the deficiencies of Mishra et al. at least with respect to node-specific configuration files.

Accordingly, even if the references are combined as suggested in the Office Action, the combination fails to establish prima facie obviousness with respect to independent claim 1, at least because the combination fails to include node-specific configuration files.

Dependent claims 3-6 and 13-16 depend directly or indirectly from independent claim 1, each including by its dependency all of the limitations of independent claim 1. Accordingly, even if the references are combined as suggested in the Office Action, dependent claims 3-6 and 13-16 are not obvious in view of the combination at least for the reasons argued above with respect to independent claim 1.

Independent claims 17 and 21 each recite similar limitations as independent claim 1 at least with respect to node-specific configuration files. Thus, even if the references are combined as suggested in the Office Action, independent claims 17 and 21 are not obvious in view of the combination for at least the reasons argued above with respect to independent claim 1.

Dependent claims 18-20 depend directly or indirectly from independent claim 17 and dependent claims 23-31 and 33 depend directly or indirectly from independent claim 21. By their dependency, each of dependent claims 18-20, 23-31, and 33 include all of the limitations of its respective base claim and is therefore allowable for reasons set forth above with respect to the respective base claim.

Claims 2 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mishra et al., in view of McDaniel et al. and further in view of Rothschild as applied to claim 1, and further

in view of the article by Lian et al. ("Time Delay Modeling And Sample Time Selection For Networked Control Systems"). Applicants traverse for reasons set forth below.

Dependent claims 2 and 22 depend from independent claims 1 and 21, respectively, each including by its dependency all of the limitations of the respective independent claim. Lian et al. fails to cure the deficiency of the combination cited above with respect to independent claims 1 and 21. Namely Lian et al. fails to teach or suggest at least the concept of delivering node specific configuration files. Accordingly, even if the references are combined as suggested in the Office Action, dependent claims 2 and 22 are not obvious in view of the combination at least for the reasons argued above with respect to independent claims 1.

Claims 11-12 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mishra et al., in view of McDaniel et al., and further in view of Rothschild as applied to claim 1 above, and further in view of the article by Hogg et al. ("A Photometricity and Extinction Monitor at the Apache Point Observatory"). Applicants traverse for reasons set forth below.

Dependent claims 11-12 depend directly or indirectly from independent claim 1, and by their dependency include all of the limitations of claim 1. Dependent claim 32 depends indirectly from independent claim 21, and by its dependency includes all of the limitations of claim 21.

As an initial matter, the combination of Hogg et al. with the other references as suggested in the Office Action is improper, at least because Hogg et al. is non-analogous art. According to §2141.01 of the M.P.E.P., in order to rely on a reference as a basis for rejection, "the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the invention was concerned. Hogg et al. is directed to an unsupervised software "robot" that automatically and robustly reduces and analyzes CCD observations of photometric standard stars. (Abstract). Applicants' invention as described in ¶0011 provides a secure network in which at least one node therein generates and distributes to each node an intelligent agent module and a set of node-specific configuration files. Hogg et al. is directed to a software robot that reduces and analyzes image data. In Section 13 relied upon in

the Office Action, Hogg et al. discusses archived output data from the photometricity monitor robot. Applicants fail to see how Hogg et al. could be construed as either in the field of applicants' endeavor, or reasonably pertinent to the particular problem with which applicants' invention is concerned.

Even if Hogg et al. were combined with the other references as suggested in the Office Action, Hogg et al. fails to cure the deficiency of the combination cited above with respect to independent claims 1 and 21. Accordingly, even if the references are combined as suggested in the Office Action, dependent claims 11-12 and 32 are not obvious in view of the combination at least for the reasons argued above with respect to independent claim 1.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 50-3431. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 50-3431. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 50-3431.

Respectfully submitted,

Date: May 3, 2007

By _____

FOLEY & LARDNER LLP
111 Huntington Avenue
Boston, Massachusetts 02199
Telephone: (617) 342-4000
Facsimile: (617) 342-4001

Ralph Trementozzi,
Registration No. 55,686 for
Mark G. Lappin,
Registration No. 26,618
Attorney for Applicants